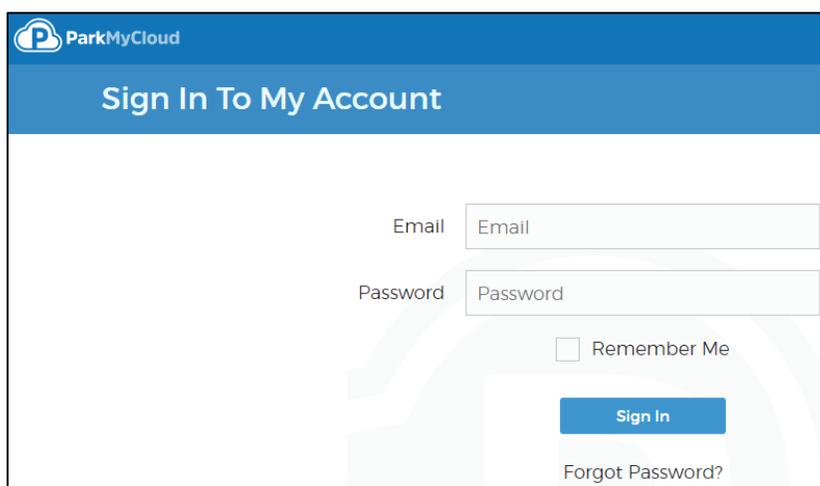


Configuring ParkMyCloud

Configuring ParkMyCloud for SSO enables administrators to manage their users using Citrix Gateway. Users can securely log on to ParkMyCloud using their enterprise credentials.

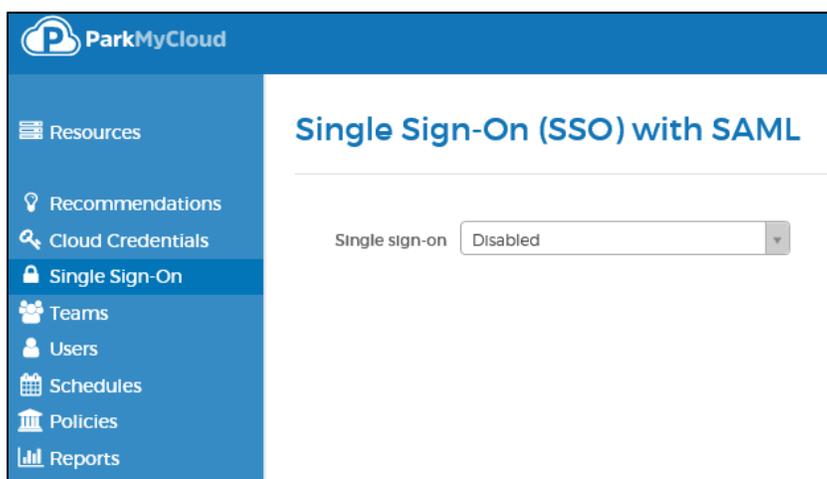
To configure ParkMyCloud for SSO through SAML, follow the steps below:

1. In a browser, type <https://console.parkmycloud.com/> and press **Enter**.
2. On the Login page, type your credentials, and click **Sign In**.



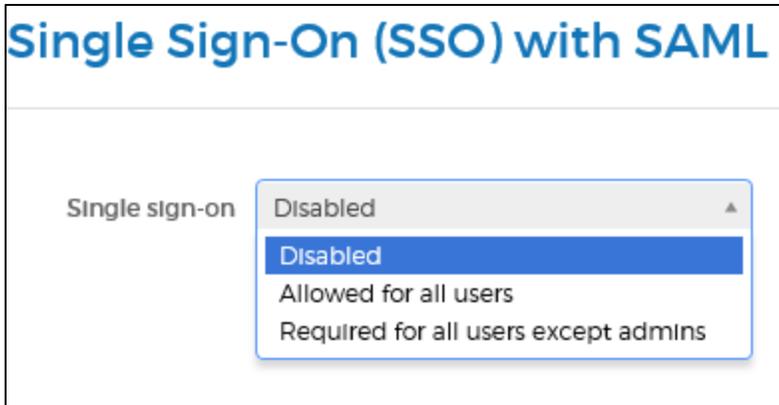
The screenshot shows the ParkMyCloud login interface. At the top left is the ParkMyCloud logo. Below it is a blue header with the text "Sign In To My Account". The main content area contains a form with two input fields: "Email" and "Password". Below the "Password" field is a checkbox labeled "Remember Me". A blue "Sign In" button is positioned below the "Remember Me" checkbox. At the bottom right of the form area is a link that says "Forgot Password?".

3. On the Landing page, click **Single Sign-On** in the top left pane.



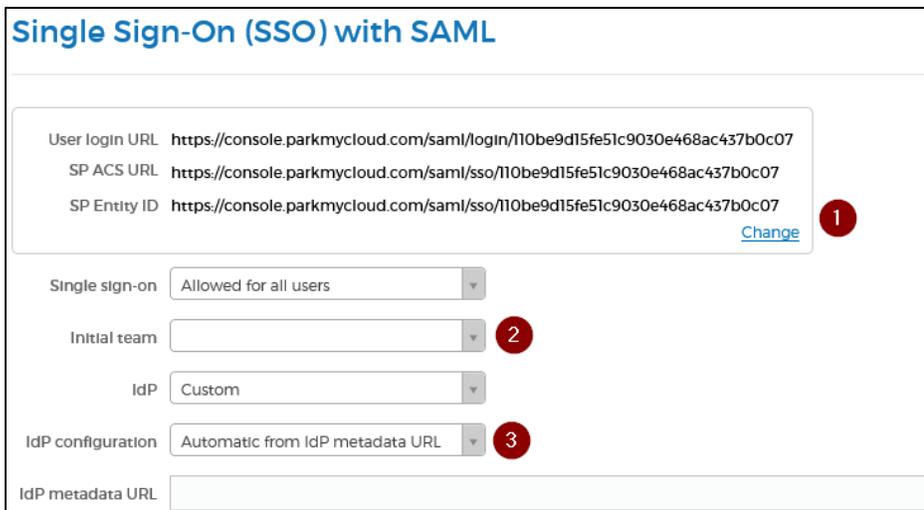
The screenshot shows the ParkMyCloud configuration page for Single Sign-On (SSO) with SAML. The top left corner features the ParkMyCloud logo. A blue sidebar on the left contains a menu with the following items: "Resources", "Recommendations", "Cloud Credentials", "Single Sign-On" (which is highlighted), "Teams", "Users", "Schedules", "Policies", and "Reports". The main content area has the title "Single Sign-On (SSO) with SAML". Below the title is a label "Single sign-on" followed by a dropdown menu currently set to "Disabled".

4. From the Single sign-on drop-down list, select **Allowed for all users** option.



The Single Sign-On with SAML page appears.

5. On the Single Sign-On with SAML page, specify the following information:



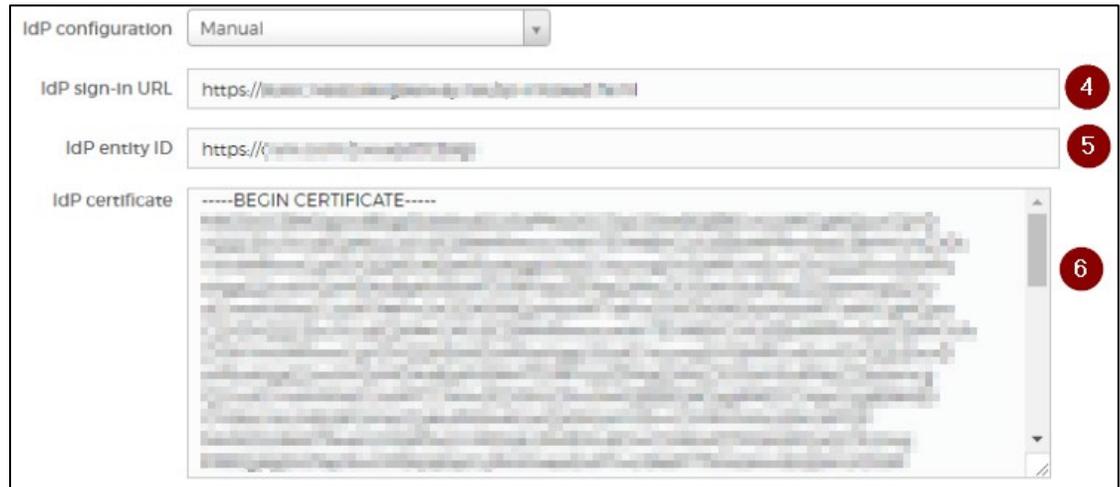
- i. In the URL field, click **Change**.



In the **Unique name** field, type your domain name.

- ii. **Initial Team:** From the drop-down list, select the appropriate option.

- iii. **IdP configuration:** From the drop-down list, select **Manual**. The IdP configuration fields are displayed.



- iv. **IdP sign-in URL:** Enter the IdP URL, SAML 2.0 endpoint, for example, <https://example.com/saml/login>
- v. **IdP Entity ID:** Enter the IdP entity ID URL.
- vi. **IdP certificate:** To upload your IdP certificate, follow the steps below:
 - a. Remotely access your NetScaler instance using PuTTY.
 - b. Navigate to /nsconfig/ssl folder (using shell command `cd /nsconfig/ssl`) and press **Enter**.
 - c. Type `cat <certificate-name>` and press **Enter**.

```

1  -----BEGIN CERTIFICATE-----
2  MIIFPzCCBCegAwIBAgIQApjY189Tw/6/mHRS5nGDUzAMBgqhkiG9w0BAQsFADBN
3  NQs=
4  alic
5  NTg
6  BAe
7  LjE
8  ADC
9  yVj
10 Kjf
11 vde
12 RKz
13 RYC
14 MBa
15 +Cc
16 Y2V
17 BBY
18 LyS
19 OjE
20 NDC
21 dC5
22 GGH
23 Y2h
24 dDA
25 PAc
26 +Xz
27 gSf
28 c+r
29 UOZLrXmupreLcnaJjorJiWlCzckp0u9TaqenWwqLNDQ04Iz/mWz0qAzy4ND
30 6ED5
31  -----END CERTIFICATE-----
32

```

- d. Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

6. Click **Save Changes**.

The SSO configuration is completed.